Fortunately, this code-breaking effort was undertaken by contest participants as part of an international challenge instead of by hackers or thieves preying on a vulnerable, unsuspecting target. It is truly scary to see how easy it is for someone's medical, financial, or personal records to be accessed and read by unauthorized persons. Ironically, the decoded message read, "It's time for those 128-, 192-, and 256-bit keys."

This feat proves what many in Congress have been stating for some time, that 56-bit encryption can no longer protect individual or corporate computer files from unauthorized access. Yet, 56- bit encryption continues to be recognized as the government standard and U.S. companies can only sell advanced encryption software and hardware to a finite community abroad. Let us be clear; the Administration's export regime affects American citizens everywhere. Whether you communicate via the Internet, or work in the technology business, you are likely to be adversely affected by the Administration's current encryption policy. A policy that does not allow the sale of strong encryption to energy suppliers, telecommunication providers, the transportation industry, human rights organizations and the vast majority of legitimate and responsible business entities and consumers throughout the globe. Ultimately, this approach promotes the use and development of weak encryption. While I welcome the White House's recent announcement to relax some export controls, the Administration's proposal simply does not go far enough.

Mr. President, it is encouraging that the Minority Leader has actively engaged himself on the encryption issue. In a floor speech last July, Senator DASCHLE agreed that America's encryption policy needs to strike a balance between privacy protections and national security and law enforcement interests. The Minority Leader recognizes that the development and use of strong encryption products promote international commerce and Internet use as well as ensure privacy and aid national security. Senator DASCHLE is also equally alarmed that, "maintaining existing encryption policies will cost the U.S. economy as much as $96 billion over the next 5 years . . ." I agree with Senator DASCHLE's comments that the Administration needs to articulate and advance an encryption agreement that is "good for consumers, good for business, and good for law enforcement and national security." Similarly, we agree that it is time to move beyond endless discussion and debate and on to a balanced and complete solution.

Mr. President, with every passing month, consumers across the globe turn to foreign suppliers for their advanced encryption needs. If a solution that reverses this trend is not found soon, then America's computer industry will fall so far behind its foreign competitors that U.S. suppliers will lose forever their technology market share to European, Asian, and other foreign manufacturers. Congress and the Administration cannot allow this happen.

As Senator DASCHLE pointed out, the computer industry and privacy groups are serious about reaching a compromise on encryption. In May, for example, Americans for Computer Privacy (ACP), a technology policy group, submitted a seven-point proposal to the Administration which would provide U.S. manufactures the ability to sell the kind of encryption technology that is already widely available abroad. In July, an industry consortium announced the "Private Doorbells" proposal to assist law enforcement. This proposal was a reasonable attempt to find an alternative to the White House's call for a national key escrow framework. Fortunately, the Administration finally appears to recognize that a third party key recovery system is technically unworkable and unnecessary.

I believe Congress is still interested in modernizing the Nation's encryption policy based on current realities. As Senator DASCHLE observed, several cryptography bills have been offered during this session. Clearly though, they are not all created equal. Some of these legislative proposals would turn back the clock by putting controls on domestic encryption where no such controls currently exist. Others would completely sacrifice constitutional protections by allowing law enforcement to read personal computer files without a court order and without the target ever knowing their files had been accessed. There are also proposals that would require an expensive, technically unworkable key escrow system. Finally, some members advocate linking encryption with other technology issues which could in the end result in no legislation being passed at all.

The encryption debate cannot be resolved by settling on a specific bit-length, giving particular industry sectors export relief while denying others the same, or by sanctioning one technical solution over another. Moreover, this debate will not be resolved by building secret backdoors, frontdoors or any doorways into encryption software.

Mr. President, I look forward to working further with Senator DASCHLE, my colleagues from both sides of the aisle, the Administration, and the computer industry to help close the gaps that still exist. As the Minority Leader recognizes, this is not about politics or partisanship. This is an urgent matter that requires us all to work together to forge an appropriate solution. One that balances the needs of industry, consumers, and the law enforcement and intelligence communities. In the end, we must have a consensus solution that brings America encryption policy into the 21st Century.

COMMENDING THE CENTER FOR SUSTAINABLE URBAN NEIGHBORHOODS

Mr. FORD. Mr. President, all across America, people from every walk of life carry a vision in their heads and in their hearts of the perfect community—of the kind of place where they can raise their children and their children can in turn raise their children.

There's no doubt that everyone's picture would look different, based on our own experience. But I feel certain they would have many elements in common. We want safe neighborhoods. We want to be economically secure. And we want to keep our families healthy. These are the building blocks of a liveable community, and the City of Louisville has played an important role in helping to put them into place, serving as a model for inner-city revitalization.

The city has rehabilitated and built hundreds of housing units, they've created new jobs and businesses, and more families are building stable, productive lives. East Russell, an inner-city Louisville Neighborhood, has seized the nation's attention by creating a renaissance in that part of the city, bringing it new life and vitality. Rightfully so, this revitalization project has received attention by mayors and elected officials all over the United States.

The University of Louisville's Sustainable Urban Neighborhoods (SUN) is devoted to making inner city neighborhoods healthy and safe places to live. The project is located at the Center for Urban and Economic Research at the University of Louisville. One of the biggest accomplishments of this project has been building affordable houses for residents with a strong cooperative effort by the entire staff, including the University of Louisville, CityBank, and Telesis, along with many community organizations.

Mr. President, the SUN staff—including its Director, Dr. John Gilderbloom and students from the University of Louisville —and SUN community partners have already done so much to strengthen our inner city communities and boost the hopes and spirits of the people living there.

I would ask that my colleagues join me today in commending their work to make our cities "dream places" to live and for their continued commitment to the greater community. And as they host their conference the week of October 15th through the 17th, we wish them the best of luck in their continued efforts.

RETIREMENT OF SENATOR DIRK KEMPTHORNE

Mr. THURMOND. Mr. President, while each of us is looking forward to adjournment so that we may go home and spend time with our constituents and being closer to our family and friends, the end of the 105th Congress is a somewhat bittersweet occasion as